90 Rec'd PCT/PTO 15 MAY 20

FORM PTO-1390 (REV 5-93)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NO. 108269-00005
	TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	DATE: May 15, 2001
		U.S. APPLN. NO. (IF KNOWN, SEE 37 CFR 1.5) 09/831368

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/JP99/06365	November 15, 1999	November 16, 1998

TITLE OF INVENTION: NETWORK AUTHENTIFICATION SYSTEM AND METHOD THEREOF

APPLICANT(S) FOR DO/EO/US: Kazuhiro AIHARA (Tokyo, Japan); Kuniaki TANEZAKI (Saitama, Japan); Masakatsu TSUKAMOTO (Tokyo, Japan); and Tamami YAMADA (Tokyo, Japan)

1. XX This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
(THE BASIC FILING FEE IS ATTACHED)

2. __ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.

3. XX This express request to begin national examination procedures (35 U.S.C. 371(f) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT articles 22 and 39(1).

4. __ A proper demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. XX A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. __ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. XX has been transmitted by the International Bureau.
   c. __ is not required, as the application was filed in the United States Receiving Office (RO/US)

6. XX A translation of the International Application into English (35 U.S.C. 371(c)(2)).

7. __ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. __ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. __ have been transmitted by the International Bureau.
   c. __ have not been made; however, the time limit for making such amendments has NOT expired.
   d. __ have not been made and will not be made.

8. __ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. __ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. __ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. XX An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

12. __ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. __ A FIRST preliminary amendment.
__ A SECOND or SUBSEQUENT preliminary amendment.

14. __ A substitute specification.

15. __ A change of power of attorney and/or address letter.

16. XX Other items or information:
Drawings (Figs. 1 - 19; 15 sheets); Japanese Language PCT Request Form (PCT/RO/101); Japanese Language PCT/IB/308; Copy of First Page of International Publication No. WO 00/29965; International Search Report (Form PCT/ISA/210)

U.S. APPLN. NO. (IF KNOWN, SEE 37 C.F.R. 1.50) 09/831368	INTERNATIONAL APPLICATION NO. PCT/JP99/06365	ATTORNEY DOCKET NO. 108269-00005 DATE: May 15, 2001

17. XX The following fees are submitted:
Basic National Fee (37 CFR 1.492(a)(1)-(5):
Search Report has been prepared by the EPO or JPO.....$860.00
International preliminary examination fee paid to USPTO (37 CFR 1.482)...$690.00
No international preliminary examination fee paid to USPTO (37 CFR1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2))....$710.00
Neither international preliminary examination fee (37 CFR 1.482) or international search fee (37 CFR 1.445(a)(2)) paid to USPTO.....$1,000.00
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00

	CALCULATIONS	PTO USE ONLY
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of $130.00 for furnishing the oath or declaration later than _ 20 _ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

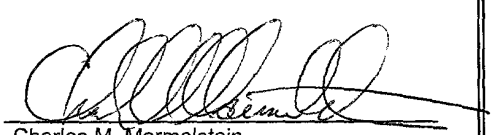
Claims	Number Filed	Number Extra	Rate		
Total Claims	11 - 20 =	0	X $ 18.00	$ 0	
Independent Claims	4 - 3 =	1	X $ 80.00	$ 80.00	
Multiple dependent claim(s) (if applicable)			+ $270.00	$ 270.00	
TOTAL OF ABOVE CALCULATIONS =				$ 1,210.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$ 1,210.00	
Processing fee of $130.00 for furnishing the English translation later than _ 20 _ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 1,210.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$	
				Amount to be refunded	$
				Charged	$ 1,210.00

a. ___ A check in the amount of $_____ to cover the above fees is enclosed.
b. XX Please charge my Deposit Account No. 01-2300 in the amount of $ 1,210.00 to cover the above fees referencing our docket no. 108269-00005. A duplicate copy of this sheet is enclosed.
c. XX The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 01-2300.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

ARENT FOX KINTNER PLOTKIN & KAHN, PLLC
1050 Connecticut Avenue, N.W.
Suite 600
Washington, D.C. 20036-5339
Telephone No. (202) 857-6000
Fax No: (202) 638-5000



Charles M. Marmelstein
Reg. No. 25,895

CMM:mmg

09/831368

15/PRTS

JC08 Rec'd PCT/PTO 15 MAY 2001

DESCRIPTION

NETWORK AUTHENTIFICATION SYSTEM AND METHOD THEREOF

Technical Field

The present invention relates to a security technique in a network for a commercial purpose such as Internet, etc..

Background Arts

As the Internet has increasingly been utilized for commercial purposes, it is required that a security technique of the network be promptly established.

That is, the Internet deals with data communications using an open protocol based on TCP/IP (Transmission Control Protocol/Internet Protocol), wherein a confidentiality of the data communications is not fundamentally schemed.

Such being the case, there were proposed a multiplicity of techniques for ensuring a data security between a user terminal and a server by use of a variety of encryption techniques such as a public key, etc..

In the cipher communications described above, it has been a general practice that a specific piece of encrypted data is transmitted to the server from the user terminal, and the server decrypts the encrypted data and authenticates a validity f the user concerned.

The authentication server itself is, however, disposed in a open environment on the Internet, and, even if a firewall is established, the situation is that whoever knows an address

TECHNICAL SECTION

of the server itself.

Namely, there can not be denied such a possibility that the authentication server, of which the address is known, therefore always becomes a target of hackers and crackers.

Further, an evil third party intercepts the encryption communication and resumes the data communications with the server, thus, so to speak, pretending to be a true user. There might also be a possibility in which a credit card etc. is illegally used on the network.

It is a technical object of the present invention, which was devised in view of the above point, to provide a system for ensuring a high security on networks by enhancing a confidentiality of an authentication server itself, using in a disposable form a program for a user to inputting data for authentication, and distributing this program to a user terminal.

Disclosure of the Invention

According to a first means of the present invention, a network authentication system comprises an intermediary server for, with respect to a user terminal inputting data, relaying this item of data, and an authentication server for giving authentication to this item of data, wherein the authentication server outputs encryption information to the intermediary server with an input of a first item of data on the user terminal serving as a trigger, and the intermediary server generates an encryption program for encrypting a second item of data inputted from the user terminal on the basis of the encryption

information received from the authentication server, and distributes this encryption program to the user terminal.

The present invention has a characteristic point of thus actualizing the [intermediary authentication system].

That is, a confidentiality of the authentication server can be enhanced by processing via the intermediary server. Namely, an address itself of the authentication server can be kept confidential.

Further, the intermediary server is provided with encryption information possessed by the authentication server, and the intermediary server generates an encryption program on the basis of this item of intrinsic encryption information. The second data is, when inputted from the user terminal, encrypted by this encryption program. Herein, the encryption program may be generated by a JAVA applet.

Note that the user terminal is not limited to a terminal device taking a form of its being installed indoors such as a personal computer, etc. and may be a mobile computer, a PDA (Personal Data Assistant) etc. connected to a movable telephone and incorporating a terminal function. Further, a movable telephone (such as an [i-mode terminal] made by NTT DOCOMO Co., Ltd.) itself, which has an Internet terminal function, may be used.

According to a second means of the present invention, in the first means, the encryption information is an encryption function, and the authentication server evaluates a validity of a session given from the user terminal by comparing the second

data encrypted by the encryption program with what the second data possessed by the authentication server itself is encrypted by the encryption function.

The encryption function is not necessarily single, and the confidentiality by the encryption is made by far higher by preparing a plurality of functions.

According to a third means of the present invention, in the first or the second means, the encryption information changes per session to the intermediary server from the user terminal.

For example, pieces of date/hour information of a mechanical timer of the authentication server are used as parameters, whereby the encryption information different per session can be generated. With this contrivance, even if a third part intercepting the data given from the user terminal illegally accesses the intermediary server, the encryption information has already changed, and hence the fraudulent third party is unable to receive a valid authentication from the authentication server, with the result that the confidentiality can be kept.

According to a fourth means of the present invention, in the first means, the first data is a user's ID, and the second data is a password. The present invention can be applied to a transfer of password information required to have a high confidentiality in confirmation of the number of acquired points of, e.g., a credit card.

According to a fifth means of the present invention, in

the second means, the encryption information is an encryption key for specifying an encryption function among a plurality of encryption functions possessed by the intermediary server instead of the authentication server.

In this case, the same function table is provided in both of the authentication server and the intermediary server, and it is feasible to specify the encryption function to be adopted from the table with the encryption key.

According to a sixth means of the present invention, a network authentication method comprises a step of making an intermediary server relay a first item of data received from a user terminal to an authentication server, a step of generating encryption information on the basis of the first data and transmitting the same encryption information to the intermediary server, a step of reading a second item of data possessed by the authentication server, corresponding to the first data, and encrypting the second data with the encryption information, a step of making the intermediary server generate an encryption program for encrypting the second data inputted in the user terminal on the basis of the encryption information and distribute the encryption program to the user terminal, a step of encrypting the second data inputted by the encryption program in the user terminal, and a step of comparing the second data encrypted in the user terminal with the second data encrypted in the authentication server.

In this means also, the confidentiality of the authentication server can be enhanced by processing via the

intermediary server. That is, the address itself of the authentication server can be kept confidential. Further, the intermediary server is provided with the encryption information possessed by the authentication server, and the intermediary server generates the encryption program on the basis of this item of intrinsic encryption information. The second data is, when inputted from the user terminal, encrypted by this encryption program. Herein, the encryption program may be generated by the JAVA applet.

According to a seventh means of the present invention, in the sixth means, the encryption information changes per session to the intermediary server from the user terminal.

For instance, pieces of date/hour information of the mechanical timer of the authentication server are used as parameters, whereby the encryption information different per session can be generated. With this contrivance, even if the third part intercepting the data given from the user terminal illegally accesses the intermediary server, the encryption information has already changed, and hence the fraudulent third party is unable to receive a valid authentication from the authentication server, with the result that the confidentiality can be kept.

According to an eighth means of the present invention, there is provided a storage medium stored with a program comprising the steps described in the sixth means.

Herein, the storage medium embraces all kinds of mediums having optical, magnetic and magneto-optic recording means, and

may include an optical disk, a magneto-optic disk, a magnetic tape, or cartridge, a cassette and a card which accommodate these mediums.

According to a ninth means of the present invention, the authentication server generates intrinsic information to a processing request with an input of the processing request on the user terminal serving as a trigger, and the intermediary server provides the user terminal with an input interface generated based on the intrinsic information.

The processing request implies an act of being transmitted by a user pushing a button displayed on, e.g., an Internet browser etc. through a mouse. The intrinsic information generated by the authentication server implies , e.g., an accept number and an encryption method which correspond to the processing request concerned.

According to a tenth means of the present invention, in the ninth means, an execution program functioning on the user terminal is prepared as the input interface, the execution program accepts an input of two or more pieces of user information, and the two or more pieces of user information inputted are encrypted and transmitted to the intermediary server.

The execution program is, e.g., the JAVA applet, and the user information implies a card number and a password which are inputted on this applet. These pieces of user information are encrypted on the applet and transmitted via the intermediary server to the authentication server.

Brief Description of the Drawings

FIG. 1 is a schematic view showing a system architecture in an embodiment of the present invention;

FIG. 2 is an explanatory view showing contents of an accept database;

FIG. 3 is an explanatory view showing contents of an authorized database;

FIG. 4 is a block diagram showing functions of an intermediary server and of an authentication server in an accept process in the embodiment thereof;

FIG. 5 is a block diagram showing functions of the intermediary server and of the authentication server in an authentication process in the embodiment thereof;

FIG. 6 is a block diagram showing procedures of generating an HTML file and an encryption applet provided to a user terminal in the embodiment thereof;

FIG. 7 is an explanatory view showing source codes of the HTML file provided to the user terminal in the embodiment thereof;

FIG. 8 is a block diagram showing a modified example of a method of generating the encryption applet in the intermediary server in the embodiment thereof;

FIG. 9 is an explanatory view (1) showing an encryption table in the embodiment thereof;

FIG. 10 is an explanatory view (2) showing the encryption table in the embodiment thereof;

FIG. 11 is an explanatory view (3) showing the encryption table in the embodiment thereof;

FIG. 12 is an explanatory view showing a ten plate of the applet in the embodiment thereof;

FIG. 13 is a sequence diagram showing a way of transferring and receiving data between the user terminal, the intermediary server, the authentication server in the embodiment thereof;

FIG. 14 is a display screen (1) of the user terminal in the embodiment thereof;

FIG. 15 is a display screen (2) of the user terminal in the embodiment thereof;

FIG. 16 is a display screen (3) of the user terminal in the embodiment thereof;

FIG. 17 is a display screen (4) of the user terminal in the embodiment thereof;

FIG. 18 is a sequence diagram (1) showing a way of transferring and receiving data between the user terminal, the intermediary server, the authentication server in a modified example in the embodiment thereof; and

FIG. 19 is a sequence diagram (2) showing the way of transferring and receiving data between the user terminal, the intermediary server, the authentication server in the modified example in the embodiment thereof.

Best Mode for Carrying out the Invention

The present invention will hereinafter be described with

reference to the drawings.

FIG. 1 is a schematic view showing a system architecture in this embodiment.

In the present embodiment, a user terminal 1 is connected via an Internet 2 to an intermediary server 3. The intermediary server 3 is connected via a firewall server 4 to an authentication server 5 by a LAN or a WAN.

The user terminal 1 is not limited to a terminal device taking a form of its being installed indoors such as a personal computer, etc. and may be a mobile computer, a PDA (Personal Data Assistant) etc. connected to a movable telephone and incorporating a terminal function. Further, a movable telephone (such as an [i-mode terminal] made by NTT DOCOMO Co., Ltd.) itself, which has an Internet terminal function, may be used.

The authentication server 5 includes an accept database 6 and an authorizing database 7. FIGS. 2 and 3 show file formats of these databases 6, 7. To be specific, the accept database 6 is registered with an accept number given by the authentication server 5, a card number inputted by the user terminal 1, and an encryption key (which will be mentioned later on) for specifying an encryption algorithm. While the authorizing database 7 is registered with a card number registered beforehand for authentication, and with a password registered likewise beforehand.

Note that the authentication server 5 includes, other than the accept database 6 and the authorizing database 7,

though not illustrated in FIG. 1, a user information database 26 and a result-of-authentication database 27 (both of which are given in FIG. 5).

The system shown in FIG. 1 is utilized in such a way that the user inputs, for instance, a credit card number and a password through the user terminal 1, and refers to points accumulated in the credit card. A high security on communications paths is required of the credit card number and the password inputted from the user terminal 1, and besides the authentication server 5 for authenticating the card number and the password is required to keep the securities of the accept database 6 and of the authorizing database 7.

In accordance with this embodiment, in those points, a data intercepts about the credit card number and the password inputted from the user terminal 1 on the communications paths, are prevented by use of a temporary disposable program, e.g., a JAVA applet, and, with the intermediary server 3 being provided, the user terminal 1 communicates directly with this intermediary server 3, thereby making confidential an address of the authentication server 5 itself and the system architecture.

Next, respective functions of the user terminal 1, the intermediary server 3 and the authentication server 5 will be explained with reference to FIG. 4.

FIG. 4 is a block diagram showing how those functions imparted to the user terminal 1, the intermediary server 3 and the authentication server 5 work through processes in which the

user terminal 1 accesses a server program 12 of the intermediary server 3 (see FIG. 14), then picks up a card number input screen (see FIG. 15) and transmits the card number to the intermediary server 3, and a password input screen shown in FIG. 16 is displayed on the user terminal 1.

To start with, the user accesses the Internet 2 from the user terminal 1 by a method such as dial pickup IP, etc., and starts up a browser (11 (WWW lookup program) within the user terminal 1. Then, a screen shown in FIG. 14 is displayed by specifying an address of a server program 12 of the intermediary server 3 as a URL (Uniform Resource Locator).

Subsequently, the user designates the point reference on the screen shown in FIG. 14, which involves use of an input assisting device such as a mouse and so on, whereby a card number input screen shown in FIG. 15 is displayed in accordance with link information set in the [Point Reference].

Herein, when the user inputs his or her own card number (e.g., [1234]), this inputted card number (ID) is transmitted to the intermediary server 3 (step (1) in FIG. 4: the numerals with braces in this embodiment correspond to the numerals with circles in FIG. 4).

When the server program 12 of the intermediary server 3 receives the card ID, the accept Servlet 13 (which is a disposable server-side program) is actuated (step (2)), and the card ID is set in a state of queuing 14 through the accept Servlet 13 (steps (3) and (4)).

The authentication server 5 periodically checks a queue

given from the intermediary server 3 with the aid of a queue fetch function 15 (step (5)), and, upon recognizing this queue 14, fetches this queue (step (6)).

Then, the authentication server 5 starts up an authorized user/agent program (which will hereinafter be termed [authorized UA]) 16, and transmits the card number ID to this authorized UA 16 (steps (7) and (8)). The authorized UA 16 is categorized as a temporary agent program and, if the communications are disconnected for some reason by the user terminal 1, might be deleted from on the authentication server 5 after a fixed time has elapsed.

The authorized UA 16 further reads an encryption key and an encryption function from an encryption function management module 17 of the authentication server 5 (step (9)), then generates an accept number, and stores the accept database 6 with accept information (step (10)). Note that the encryption key implies key information for encryption and involve use of an encryption function alternatively taken per accessing from a plurality of encryption functions.

The following is a reason why the encryption key described above is prepared.

Namely, the card ID is fixed, and hence it can be considered that the accessing might be tried a plurality of times with the same card ID. Therefore, a fraudulent access can be prevented by preparing the plurality of encryption functions capable of actualizing the encryption key different per accessing with respect to the card ID.

Incidentally, the encryption key and the encryption functions will be explained later on referring to FIGS. 9, 10 and 11. Further, the accept number is a sequential number and reset at 12:00 am every day. Specifically, a third access on the very day is given a number [0003].

The authorized UA 16 creates the accept number given in sequence of acceptances as described above (step (10)), and stores the accept database 6 with this accept number together with the card ID and the encryption key (see FIG. 2).

Next, the authorized UA 16 indicates the intermediary server 3 to start up an intermediary user/agent (which will hereinafter be called an [intermediary UA] 20 (steps (11) and (12)).

When the intermediary UA 20 is started up within the intermediary server 3, the authorized UA 16 of the authentication server 5 transmits accept information consisting of the accept number, the card ID and the encryption function (step (13)).

The intermediary UA 20 having received this piece of accept information transmits the accept number and the encryption function to the accept Servlet 13 described above (step (14)).

The accept Servlet 13, based on this, generates an encryption applet 21 into which the accept number and the encryption function are embedded (step (15)). This encryption applet 21 is transmitted to the browser 11 of the user terminal 1 via the server program (steps (16) and (17)).

The encryption applet 21 is defined as a so-called JAVA applet and transmitted to the browser 11 of the user terminal 1 together with a HTML (Hyper Text Markup Language) file serving as an interface. FIG. 16 shows a screen of the browser 11 at that time. The HTML file for displaying this is structured of a text description as shown in FIG. 7. In this description, OTP19980812114910.class designated as APPLET CODE is a file name of the encryption applet 21. The encryption applet 21 is a so-called one-time program as well as being a temporary program used for only a session for authenticating the card ID concerned. The encryption applet 21, as described above, consists of the encryption function and the accept number given by the authentication server 5, and therefore a possibility of the identical encryption applet 21 being generated might decrease by the order of an astronomical numerical value.

Next, the functions of the intermediary server 3 and of the authentication server 5 till an authentication screen as shown in FIG.17 is displayed since the password inputted on the applet screen shown in FIG. 16 has been authenticated by the authentication server 5 via the intermediary server 3 on the browser 11 of the user terminal 1, will be explained referring to FIG. 5.

To begin with, the password inputted through the browser 11 on the user terminal 1 is encrypted by the encryption applet 21 generated for one single session as discussed above, and transmitted to the intermediary server 3 (step (2)). Even if the communications concerned might be intercepted by tracing

the circuit between the user terminal 1 and the intermediary server 3 by encrypting the password inputted by use of the encryption applet 21 limited to one single session which has been provided from the intermediary server 3, the password is unable to be used for a next session by the same card ID.

In the intermediary server 3 having received the encrypted password, an authentication Servlet 25 is started up by the server program 12, and the encrypted password is transferred to this Servlet 25 (steps (3) and (4)).

Herein, the authentication Servlet 25 carries on the accept number possessed by the accept Servlet 13 explained in FIG. 4, and transmits this accept number together with the encrypted password to the intermediary UA 20 (step (5)).

The authorizing UA 16 of the authentication server 5 issues a request for authentication to the intermediary server 3 at a fixed interval (step (1)), and, if there occurs a state where the intermediary UA 20 of the intermediary server 3 receives the accept number and the encrypted password, these pieces of information are transmitted to the authorizing UA 16 with this authentication request serving as a trigger (step (6)).

The authorizing UA 16 accesses the accept database 6 with the accept number serving as a key, and reads a card ID and an encryption key which correspond to this accept number (step (7)). Then, with a set of the card ID, the encryption key which have been thus obtained and the encrypted password, an authentication module 28 is requested to perform the

authentication (step (8)).

The authentication module 28 having accepted the authentication request reads the encryption function from the encryption function management module 17 (step (9)), and further reads the password from the authorized database 7 with the card ID serving as the key (step (10)). Then, the authentication module 28 encrypts the password read from the authorized database 7 by use of the encryption function (step (11)). The authentication module 28 compares this encrypted password with the above encrypted password received by the authorizing UA 16 (step (12)).

The authentication module 28, if those two encrypted passwords are identical with each other, answers that the authentication is OK, and reads user information from user information database 26 (step (13)). These pieces of user information may include the number of acquired points with respect to the credit card of the relevant user, and so on. Then, the authentication module 28 registers in an authenticated result database 27 the accept number, the encryption password and the user information as a result of the authentication (step (14)). With this registration, the authentication module 28 transmits the result of authentication, i.e., a result flag indicating that the authentication is OK and the user information such as the number of acquired points to the authorizing UA 16 (step (15)).

The authorizing UA 16, if the result of authentication is OK, writes the encrypted password to the accept database 6

(step (16)), , and transmits the result of authentication together with the user information to the intermediary UA 20 of the intermediary server 3 (step (17)).

The result of authentication is transmitted to the user terminal 1 via a route such as the intermediary UA 20 of the intermediary server 3 → the authentication Servlet 25 → the server program 12, and is displayed on the browser screen of the user terminal 1 (steps (18) ~ (20)).

FIG. 17 shows the screen on the display of the user terminal 1 at that time.

Next, a procedure of generating the encryption applet 21 and the HTML file provided to browser 11 explained in FIG. 4, will be described with reference to FIG. 6.

At the first onset, as discussed above, when the card ID is inputted from on the browser 11 (step (1)), the server program is started up, thereby prompting the actuation of the accept Servlet 13 (step (2)).

The accept Servlet 13, at first, selectively reads a ten plate 61 of the applet as shown in FIG. 12 (step (3)), and performs rewriting of a seed program (Seed) and outputting of an execution file (class) (step (4)), thereby generating the encryption applet 21. Then, this encryption applet 21 is supplied together with HTML data 62 created by the accept Servlet 13 to the browser 11 of the user terminal 1 through the server program 12 (steps (5) and (6)).

FIG. 7 shows specific source codes of the HTML data 62.

Next, the encryption in this embodiment will be

explained.

To start with, the encryption key is set for making the encryption applet 21 disposable with a limit to the very session. Namely, it follows that there is generated an encryption formula different per session by operating the encryption key. For this purpose, the encryption function management module 17 is provided with encryption tables A and B in which the encryption functions shown in FIGS. 9 and 10 are registered.

That is, in accordance with this embodiment, the encryption function adopted by the encryption key is specified, and this encryption key is retained within the accept database 6 of the authentication server 5 for authenticating afterward (see FIG. 5).

Referring to FIGS. 9 and 10, a parameter "a" indicates a date and obtained from a timer function incorporated into each server. In the table structure given above, when [A3] is designated as an encryption key, a third equation, i.e., [Y = aX + 3] in the table A shown in FIG. 9 is adopted. In the case of using this equation, supposing that the date concerned is, for example, 10th (a = 10), a numerical value Y obtained by multiplying an inputted numerical value X by 10 and adding 3 to the multiplied result, becomes an encryption value.

Note that the encryption key may involve use of a value of a mechanical timer of the server as a parameter so as to generate the numerical value different per session. For instance, if the functions shown in FIG. 11 are registered in the encryption table, A indicates second (4 digits) of the

mechanical timer of the server, B represents year, month and date (6 digits) of the mechanical timer of the server, and C denotes hour and minute (4 digits) of the mechanical timer of the server.

Next, the process of transferring and receiving the information between the user terminal 1, the intermediary server 3 and the authentication server 5 will be explained by use of the following specific numerical values with reference to FIG. 13 for facilitating comprehension of the encryption and the authentication in this embodiment.

Card number (ID): 1234

Accept number: 4912

Password: 9104

Encryption function: Y = 3X - 99

To begin with, when [1234] is inputted as the card number (ID) from the user terminal 1 (step 1301), the intermediary server 3 receives this card number (ID) for a relay (1302) and notifies the authentication server 5 of the same number.

The authentication server 5 obtains this card number (ID) [1234] and gives an accept number [4912] thereto. Then, an encryption method is set (1303). To be specific, an encryption function [Y = 3X - 99] and an encryption key for specifying this function are read from the encryption function management module 17 (see FIG. 4).

The intermediary server 3 obtains the accept number [4912] and the encryption function [Y = 3X - 99] from the authentication server 5 (1304), and generates the encryption

applet 21 into which the accept number and the encryption function are embedded (1305).

Next, when a password [9104] is inputted to on the user terminal 1 (1306), this is calculated based on the encryption function [Y = 3X - 99], and the authentication server 5 is notified of a result of the calculation as an encrypted password [27213] via the intermediary server 3 (1307, 1308).

On the other hand, the authentication server 5 reads, in parallel with the above processing, the encryption function [Y = 3X - 99] from the encryption function management module 17 (1309), and reads a password [9104] from the authorized database 7, in which the card number (ID) obtained in step 1303 serves as a key (1310). Then, the read password is encrypted by the encryption function [Y = 3X - 99] (1311). Then, the numerical value encrypted herein is compared with the encrypted password [27213] of which the user terminal 1 has notified (1312).

As a result, if what the password stored in the authorized database 7 is encrypted is identical with the encrypted password given from the user terminal 1, the authentication is established, and the user information retained in the authentication server 5 is supplied via the intermediary server 3 (1313) to the user terminal 1 (1314).

Note that the discussion made above has dealt with the case where the authentication server 5 notifies the intermediary server 3 of the encryption function, and the encryption applet 21 is generated, however, as shown in FIG. 8, the intermediary server 3 receives only an encryption key

801 from the authentication server 5, and the encryption applet 21 may also be generated by a combination with a function table 802 possessed by the intermediary server 3 itself.

In this case, the function table 802 held by the intermediary server 3 must be identical with the function table of the encryption function management module 17 possessed by the authentication server 5.

FIG. 18 is a sequence diagram showing how the data are transferred and received between the user terminal the intermediary server and the authentication server in a modified example of the embodiment of the present invention.

In the sequence diagram in FIG. 13, the authentication server issues the accept number after the card number has been inputted from the user terminal 1, and, based on this issuance, the intermediary server 3 generates and distributes the applet. The user terminal 1 is contrived to input the password on this applet.

By contrast, in the sequence in FIG. 18, when a processing request is made by the user terminal 1, the intermediary server generates and distributes the applet on the basis of the encryption method and the accept number given from the authentication server 5, and the user terminal 1 is contrived to input the card number and the password on this applet.

This process will be described more specifically.

To begin with, when the user clicks a processing request button displayed via the Internet browser, etc. on the user terminal 1 (step 1801), the intermediary server 3 notifies the

authentication server 5 of a purport that this processing request has been given (1802). The authentication server 5, based on this, sets the accept number and the encryption method (involving use of, e.g., the encryption function [Y = 3X - 99]) (1803). The process in this step 1803 is the same as step 1303 in FIG. 13. Herein, supposing that 4912 as an accept number is given to the authentication server 5, the intermediary server 3 is notified of this accept number and the encryption method (1805).

The intermediary server 3, based on this, generates the applet and distributes this applet to the user terminal 1 (1805).

The applet distributed from the intermediary server 3 is executed on the user terminal 1, and an input of the card number and the password from the user is accepted (1806). Herein, the password inputted is converted into an encrypted password (which is herein Y = 3X - 99 = 3 X 9104 - 99 = 27213) on the applet on the basis of the encryption method described above, and this encrypted password is transmitted to the intermediary server 3 (1807).

On the other hand, the authentication server 5 reads, in parallel with the above processing, the encryption function [Y = 3X - 99] from the encryption function management module 17 (1809), and reads target data from the authorized database 7 (1810). The target data contain the card number and the password [9104]. Then, the read password is encrypted by the encryption function [Y = 3X - 99] (1811). subsequently, the

numerical value encrypted herein is compared with the encrypted password [27213] of which the user terminal 1 has notified (1812).

As a result, if what the password stored in the authorized database 7 is encrypted is identical with the encrypted password given from the user terminal 1, the authentication is established, and the user information retained in the authentication server 5 is supplied via the intermediary server 3 (1813) to the user terminal 1 (1814).

Thus, in the modified example shown in FIG. 18, the card number and the password are inputted on the same applet to the user, and hence the user never feels a stress caused by waiting for an input screen of the password since the card number has been inputted.

Further, FIG. 18 exemplifies the example of inputting two pieces of user information such as the card number and the password on the applet in step 1806, however, the user information is not limited to these two items, and a plurality of items may also be inputted. FIG, 19 is a sequence diagram showing this example. As shown in FIG. 19, plural items of data are registered in the authorized database 7 and collated with the user information inputted.

Incidentally, the details thereof are the same as what has been explained in FIGS. 13 and 18, and the explanation is therefore omitted.

As discussed above, according to the present invention, an existence of the authentication server itself can be made

confidential by the route via the intermediary server with respect to the authenticating operation from the user terminal.

Moreover, the intermediary server provides the encryption program disposable with the limit to the very session, and the input data can be encrypted by this encryption program on the user terminal. Hence, the data communications exhibiting a high security against a leak on the communications path, can be attained.

In addition, the encryption program is categorized as the encryption program disposable with the limit to the very session, and therefore, even if a third party launches into a session based on the leaked data, the encryption program never be coincident, whereby the fraudulent access can be prevented.

Industrial Applicability

The present invention can be applied to the authentication system in a case where the user purchases commercial goods via the Internet from a terminal computer and a portable terminal, and so on.

WHAT IS CLAIMED IS:

1. A network authentication system comprising:

an intermediary server for, with respect to a user terminal inputting data, relaying this item of data; and

an authentication server for giving authentication to this item of data,

wherein said authentication server outputs encryption information to said intermediary server with an input of a first item of data on said user terminal serving as a trigger, and

said intermediary server generates an encryption program for encrypting a second item of data inputted from said user terminal on the basis of the encryption information received from said authentication server, and distributes this encryption program to said user terminal.

2. A network authentication system according to claim 1, wherein the encryption information is an encryption function, and

said authentication server evaluates a validity of a session given from said user terminal by comparing the second data encrypted by the encryption program with what the second data possessed by said authentication server itself is encrypted by the encryption function.

3. A network authentication system according to claim 1 or 2, wherein the encryption information changes per session to said intermediary server from said user terminal.

4. A network authentication system according to claim 1, wherein the first data is a user's ID, and

the second data is a password.

5. A network authentication system according to claim 2, wherein the encryption information is an encryption key for specifying an encryption function among a plurality of encryption functions possessed by said intermediary server instead of said authentication server.

6. A network authentication method comprising:

a step of making an intermediary server relay a first item of data received from a user terminal to an authentication server;

a step of generating encryption information on the basis of the first data and transmitting the same encryption information to said intermediary server;

a step of reading a second item of data possessed by said authentication server, corresponding to the first data, and encrypting the second data with the encryption information;

a step of making said intermediary server generate an encryption program for encrypting the second data inputted in said user terminal on the basis of the encryption information and distribute the encryption program to said user terminal;

a step of encrypting the second data inputted by the encryption program in said user terminal; and

a step of comparing the second data encrypted in said user terminal with the second data encrypted in said authentication server.

7. A network authentication method according to claim 6, wherein the encryption information changes per session to said intermediary server from said user terminal.

8. A storage medium stored with a program comprising:

a step of making an intermediary server relay a first item of data received from a user terminal to an authentication server;

a step of generating encryption information on the basis of the first data and transmitting the same encryption information to said intermediary server;

a step of reading a second item of data possessed by said authentication server, corresponding to the first data, and encrypting the second data with the encryption information;

a step of making said intermediary server generate an encryption program for encrypting the second data inputted in said user terminal on the basis of the encryption information and distribute the encryption program to said user terminal;

a step of encrypting the second data inputted by the encryption program in said user terminal; and

a step of comparing the second data encrypted in said user terminal with the second data encrypted in said authentication server.

9. A network authentication system comprising:

an intermediary server for, with respect to a user terminal inputting data, relaying this item of data; and

an authentication server for giving authentication to this item of data,

wherein said authentication server generates intrinsic information to a processing request with an input of the processing request on said user terminal serving as a trigger, and

said intermediary server provides said user terminal with an input interface generated based on the intrinsic information.

10. A network authentication system according to claim 9, wherein said input interface is an execution program functioning on said user terminal,

the execution program accepts an input of two or more pieces of user information, and

the two or more pieces of user information inputted are encrypted and transmitted to said intermediary server.

Abstract

When an ID is inputted from a personal computer and a mobile terminal, an authentication server is notified of this ID via an intermediary server. The authentication server , based on this ID, notifies the intermediary server of encryption information at that point of time. The intermediary server provides a user terminal with a disposable program for inputting data on the basis of the encryption information. A password inputted in the user terminal is encrypted by this program, and the authentication server is notified of the encrypted password and checks its validity. A confidentiality of the authentication server itself can be thus kept because of processing via the intermediary server. The disposable program is provided in a form such as a JAVA applet, whereby a fraudulent access by a third party intercepting a session concerned can be prevented.

FIG. 1

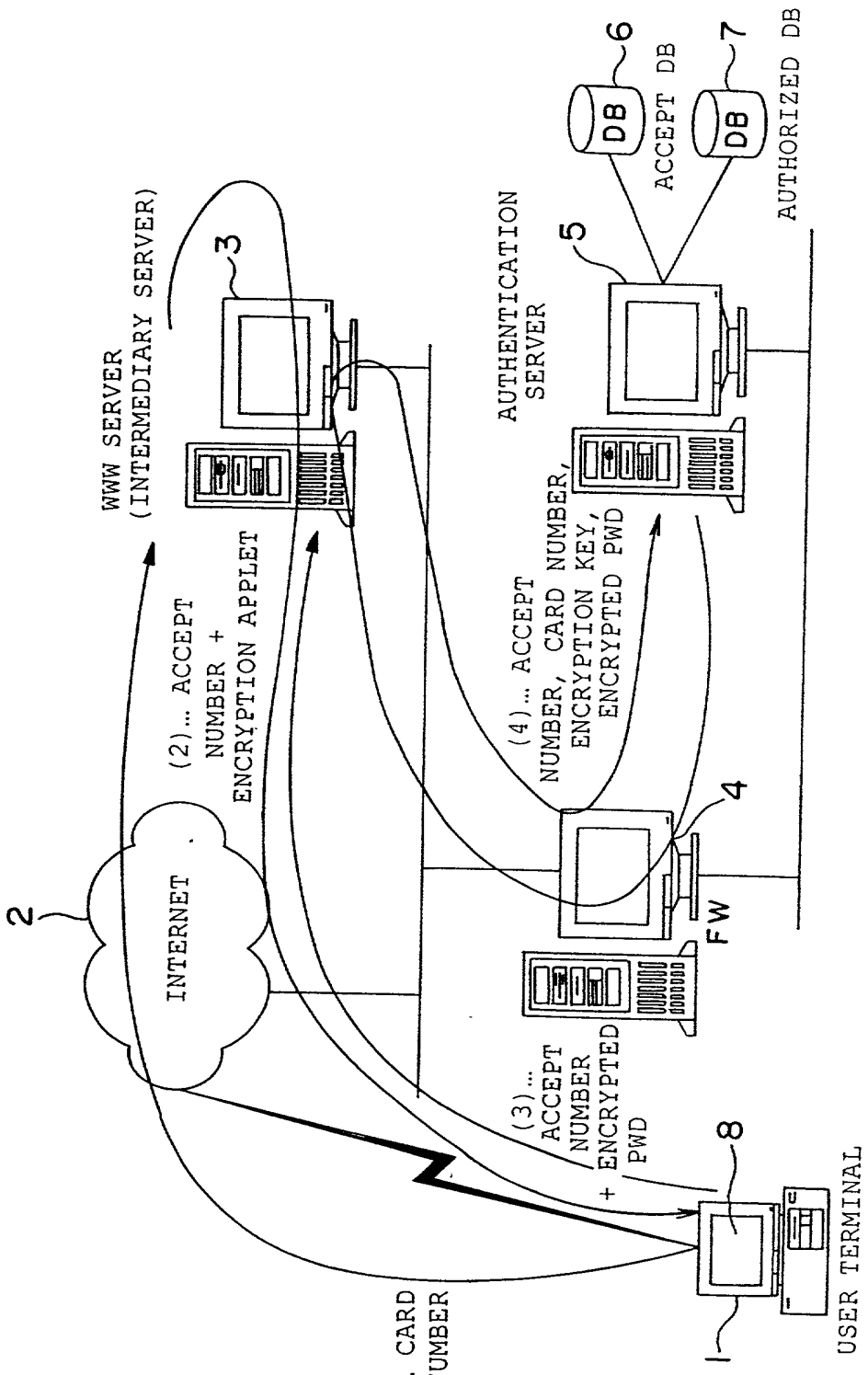

WWW SERVER
(INTERMEDIARY SERVER)
3
AUTHENTICATION
SERVER
5
6
DB
ACCEPT DB
7
DB
AUTHORIZED DB
2
INTERNET
(2)... ACCEPT
NUMBER +
ENCRYPTION APPLET
(4)... ACCEPT
NUMBER, CARD NUMBER,
ENCRYPTION KEY,
ENCRYPTED PWD
4
FW
(3)...
ACCEPT
NUMBER
+ ENCRYPTED
PWD
8
(1)... CARD
NUMBER
1
USER TERMINAL

FIG. 2

<ACCEPT DB>

ACCEPT NUMBER: ACCEPT NUMBER NUMBERED BY AUTHENTICATION SERVER
CARD ID: CARD NUMBER INPUTTED BY USER
ENCRYPTION KEY: KEY FOR SPECIFYING ENCRYPTION ALGORITHM

EDC0360 "05/15/2360

FIG. 3

<AURTHORIZED DB>.

CARD ID: PRE-REGISTERED CARD NUMBER
PASSWORD: PRE-REGISTERED PASSWORD

FIG. 4

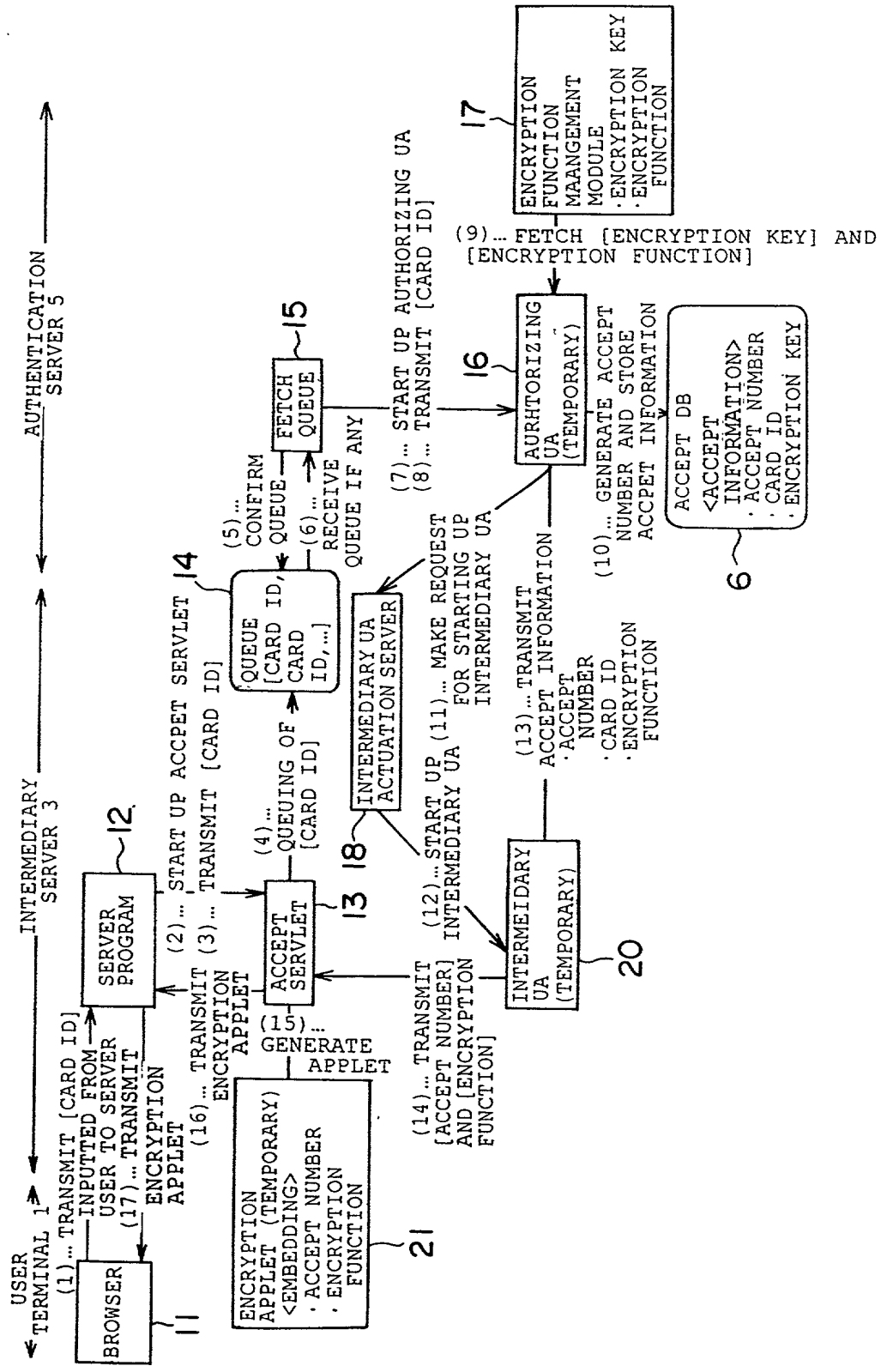

USER TERMINAL 1
INTERMEDIARY SERVER 3
AUTHENTICATION SERVER 5
(1)... TRANSMIT [CARD ID] INPUTTED FROM USER TO SERVER
(17)... TRANSMIT ENCRYPTION APPLET
BROWSER
11
SERVER PROGRAM
12
(2)... START UP ACCPET SERVLET
(3)... TRANSMIT [CARD ID]
(16)... TRANSMIT ENCRYPTION APPLET
ACCEPT SERVLET
13
(4)... QUEUING OF [CARD ID]
(15)... GENERATE APPLET
ENCRYPTION APPLET (TEMPORARY)
<EMBEDDING>
· ACCEPT NUMBER
· ENCRYPTION FUNCTION
21
QUEUE [CARD ID, CARD ID,...]
14
(5)... CONFIRM QUEUE
(6)... RECEIVE QUEUE IF ANY
FETCH QUEUE
15
INTERMEDIARY UA ACTUATION SERVER
18
(7)... START UP AUTHORIZING UA
(8)... TRANSMIT [CARD ID]
AURHTORIZING UA (TEMPORARY)
16
(9)... FETCH [ENCRYPTION KEY] AND [ENCRYPTION FUNCTION]
ENCRYPTION FUNCTION MAANGEMENT MODULE
· ENCRYPTION KEY
· ENCRYPTION FUNCTION
17
(10)... GENERATE ACCEPT NUMBER AND STORE ACCPET INFORMATION
ACCEPT DB
<ACCEPT INFORMATION>
· ACCEPT NUMBER
· CARD ID
· ENCRYPTION KEY
6
(11)... MAKE REQUEST FOR STARTING UP INTERMEDIARY UA
(12)... START UP INTERMEDIARY UA
(13)... TRANSMIT ACCEPT INFORMATION
· ACCEPT NUMBER
· CARD ID
· ENCRYPTION FUNCTION
(14)... TRANSMIT [ACCEPT NUMBER] AND [ENCRYPTION FUNCTION]
INTERMEIDARY UA (TEMPORARY)
20

FIG. 5

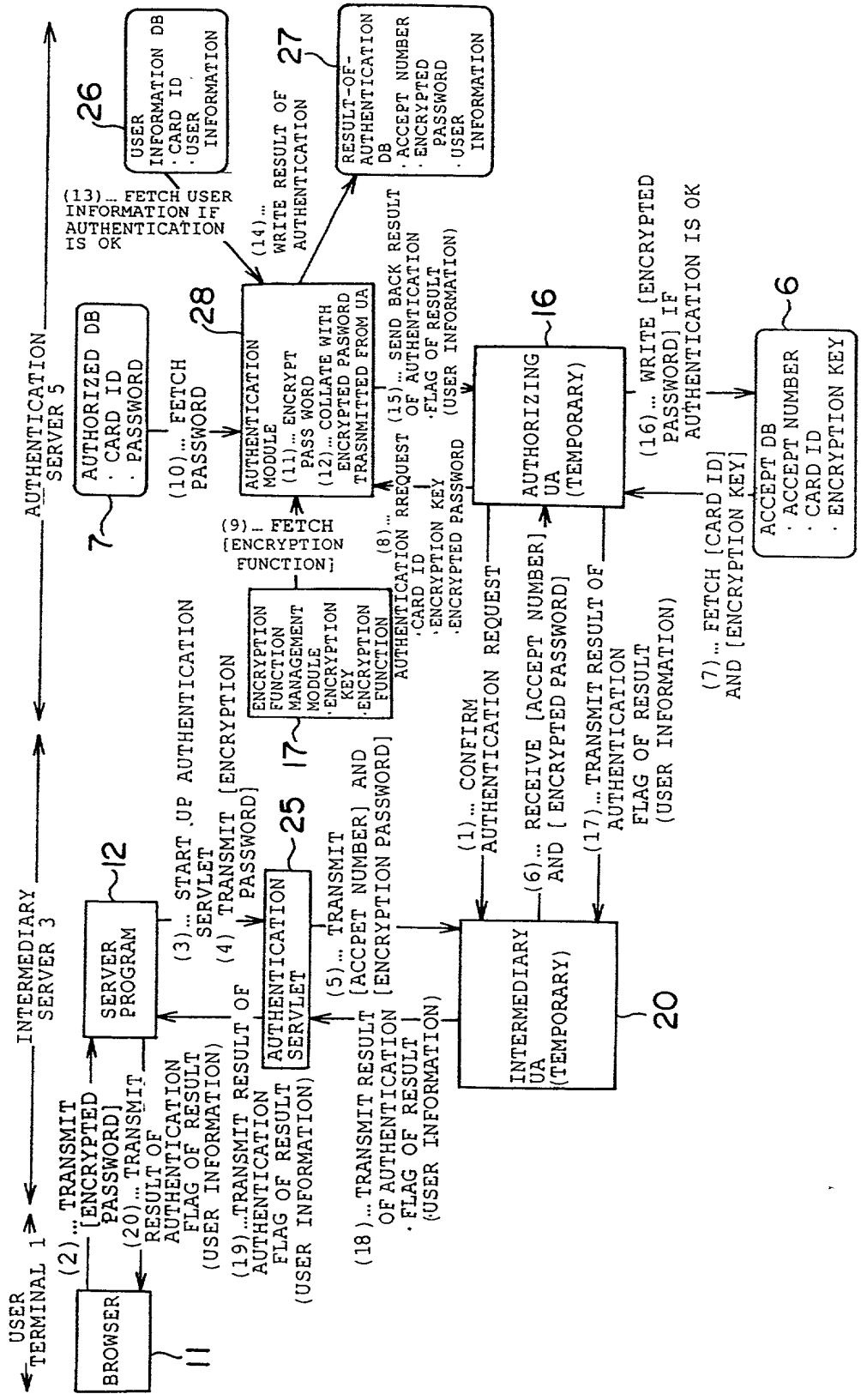

USER TERMINAL 1
BROWSER
11
AUTHENTICATION SERVER 5
INTERMEDIARY SERVER 3
SERVER PROGRAM
12
AUTHENTICATION SERVLET
25
ENCRYPTION FUNCTION MANAGEMENT MODULE
·ENCRYPTION KEY
·ENCRYPTION FUNCTION
17
AUTHORIZED DB
· CARD ID
· PASSWORD
7
AUTHENTICATION MODULE
28
USER INFORMATION DB
· CARD ID
· USER INFORMATION
26
RESULT-OF-AUTHENTICATION DB
· ACCEPT NUMBER
· ENCRYPTED PASSWORD
· USER INFORMATION
27
INTERMEDIARY UA (TEMPORARY)
20
AUTHORIZING UA (TEMPORARY)
16
ACCEPT DB
· ACCEPT NUMBER
· CARD ID
· ENCRYPTION KEY
6
(1)... CONFIRM AUTHENTICATION REQUEST
(2)... TRANSMIT [ENCRYPTED PASSWORD]
(3)... START UP AUTHENTICATION SERVLET
(4) TRANSMIT [ENCRYPTION PASSWORD]
(5)... TRANSMIT [ACCPET NUMBER] AND [ENCRYPTION PASSWORD]
(6)... RECEIVE [ACCEPT NUMBER] AND [ENCRYPTED PASSWORD]
(7)... FETCH [CARD ID] AND [ENCRYPTION KEY]
(8)... AUTHENTICATION RREQUEST ·CARD ID ·ENCRYPTION KEY ·ENCRYPTED PASSWORD
(9)... FETCH [ENCRYPTION FUNCTION]
(10)... FETCH PASSWORD
(11)... ENCRYPT PASS WORD
(12)... COLLATE WITH ENCRYPTED PASWORD TRASNMITTED FROM UA
(13)... FETCH USER INFORMATION IF AUTHENTICATION IS OK
(14)... WRITE RESULT OF AUTHENTICATION
(15)... SEND BACK RESULT OF AUTHENTICATION ·FLAG OF RESULT (USER INFORMATION)
(16)... WRITE [ENCRYPTED PASSWORD] IF AUTHENTICATION IS OK
(17)... TRANSMIT RESULT OF AUTHENTICATION FLAG OF RESULT (USER INFORMATION)
(18)... TRANSMIT RESULT OF AUTHENTICATION · FLAG OF RESULT (USER INFORMATION)
(19)...TRANSMIT RESULT OF AUTHENTICATION FLAG OF RESULT (USER INFORMATION)
(20)... TRANSMIT RESULT OF AUTHENTICATION FLAG OF RESULT (USER INFORMATION)

FIG. 6

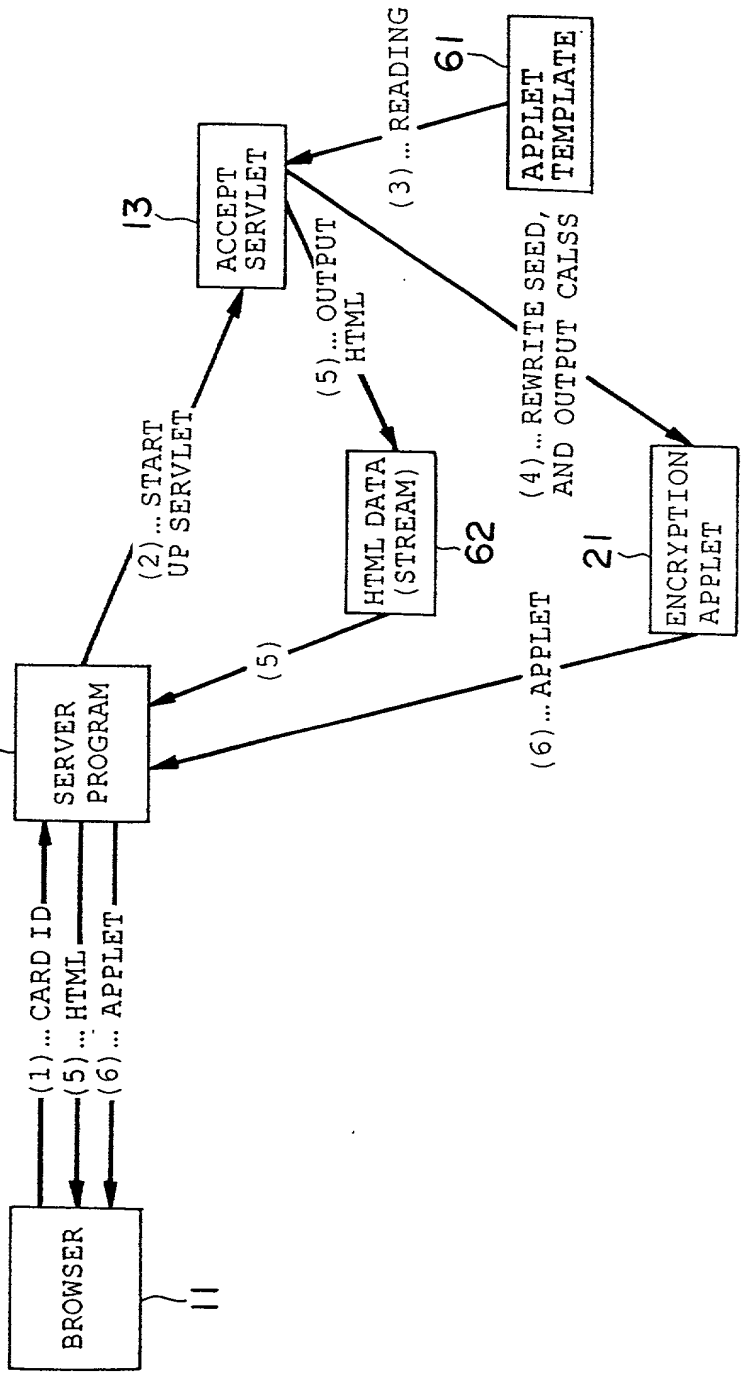

BROWSER
11
SERVER PROGRAM
12
ACCEPT SERVLET
13
APPLET TEMPLATE
61
HTML DATA (STREAM)
62
ENCRYPTION APPLET
21
(1)... CARD ID
(5)... HTML
(6)... APPLET
(2)... START UP SERVLET
(3)... READING
(4)... REWRITE SEED, AND OUTPUT CALSS
(5)... OUTPUT HTML
(5)
(6)... APPLET

FIG. 7

```
<HTML>
<HEAD>
<TITLE> PASSWORD INPUT SCREEN </TITLE>
</HEAD>
<BODY>

   . . . . . .

<APPLET CODE="OTP19980812114910.class" WIDTH=400 HEIGHT=300>
</APPLET>

   . . . . . .

</BODY>
</HTML>
```

62

FIG. 8

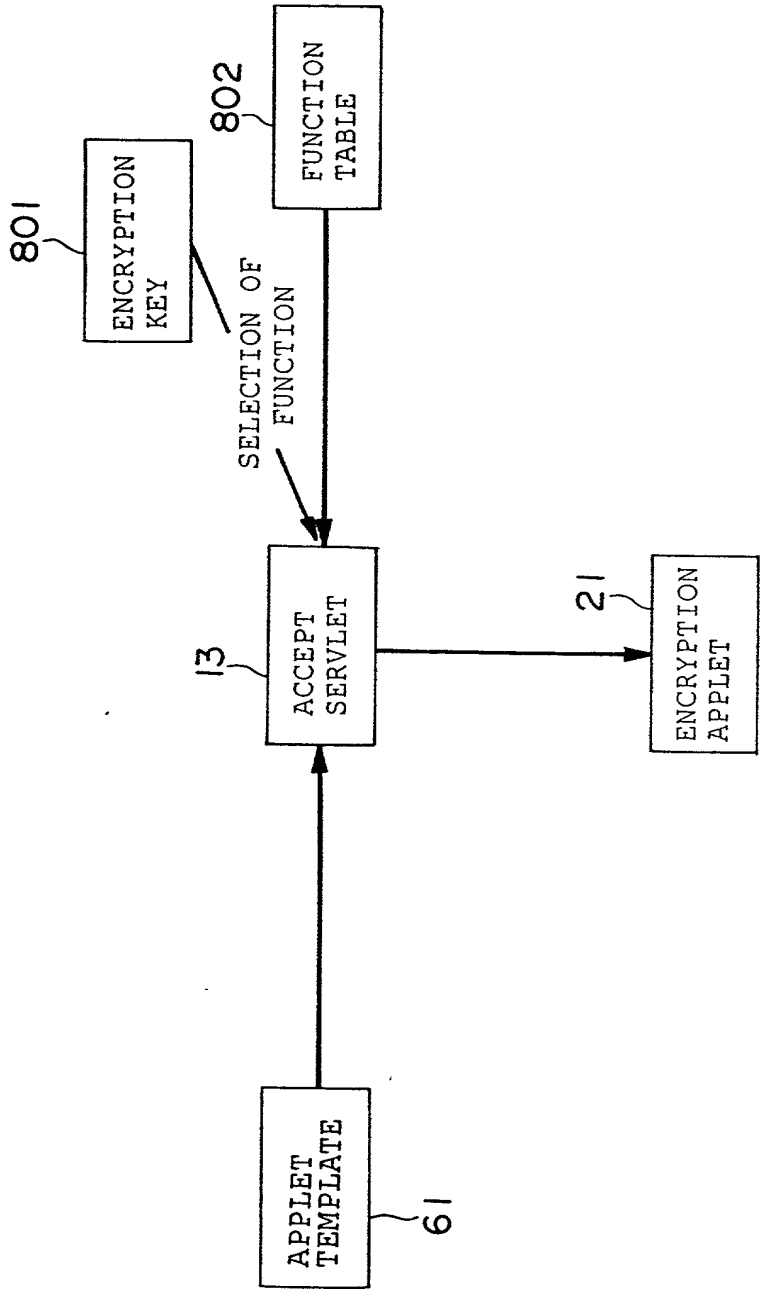

801
ENCRYPTION KEY
802
FUNCTION TABLE
SELECTION OF FUNCTION
13
ACCEPT SERVLET
21
ENCRYPTION APPLET
APPLET TEMPLATE
61

FIG. 9

table A

1	Y = aX + 2
2	Y = aX + 9
3	Y = aX + 3

a: USE DATE ON MACHINE

EFS Web 2.2.9 - 6/5/2006

FIG. 10

table B

4	Y = bX + 5
5	Y = bX + 7
6	Y = bX + 6

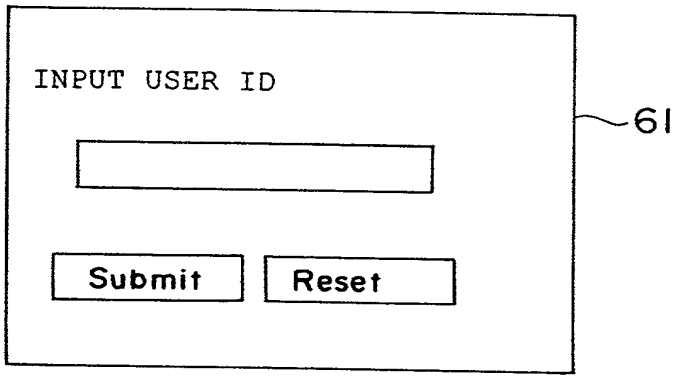
b: USE MONTH ON MACHINE

FIG. 11

LOW-ORDER ONE DIGIT OF DATE IS 1, 4, 7	Y = AX + B + C
LOW-ORDER ONE DIGIT OF DATE IS 2, 5, 8	Y = (A+B)X + C
LOW-ORDER ONE DIGIT OF DATE IS 3, 6, 9	Y = (A+C)X + B
LOW-ORDER ONE DIGIT OF DATE IS 0	Y = (A+B+C)X + A

09/831368

FIG. 12



TOKYO - 09.04.01

FIG. 13

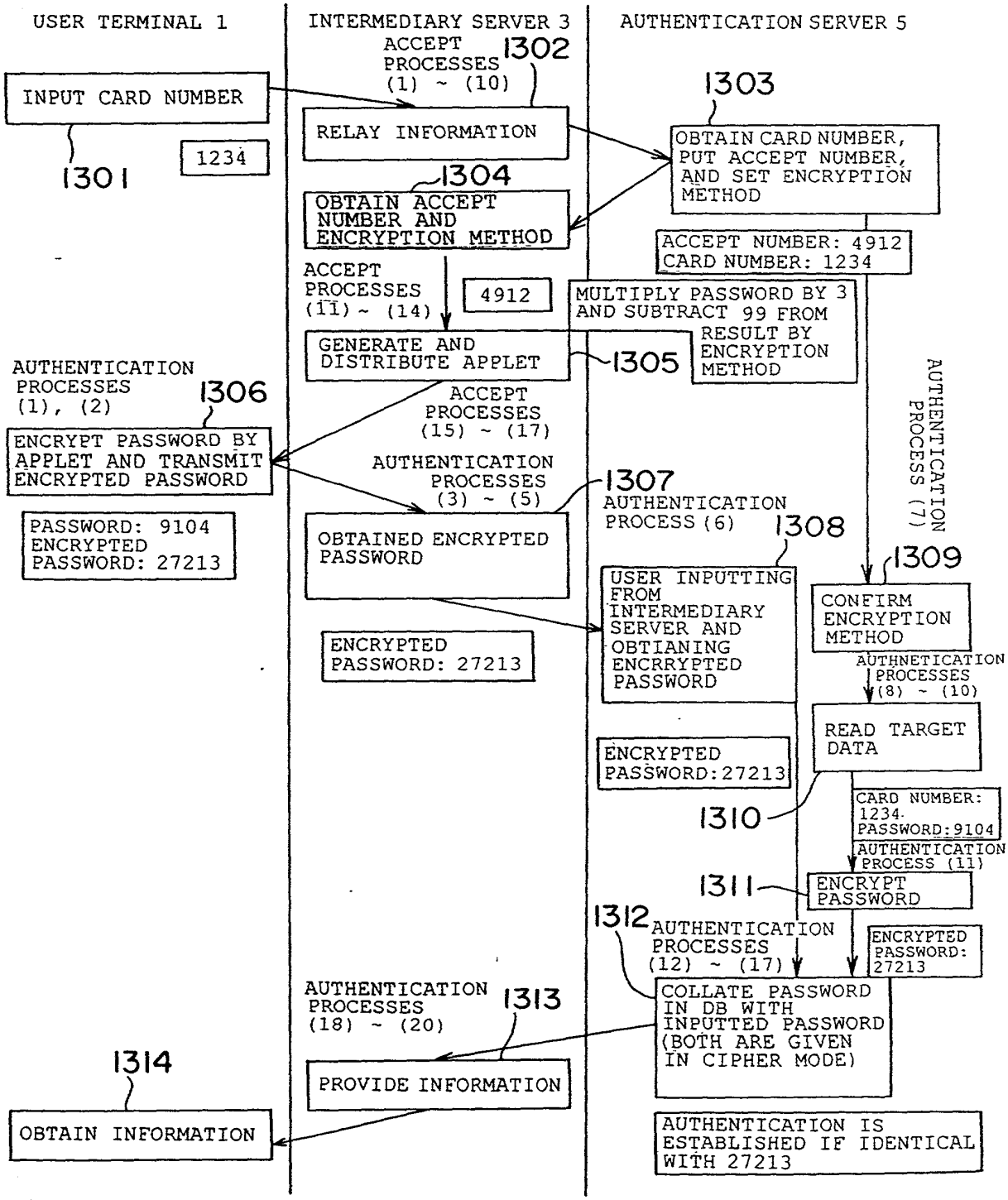

USER TERMINAL 1
INTERMEDIARY SERVER 3
AUTHENTICATION SERVER 5
ACCEPT PROCESSES (1) ~ (10)
1302
INPUT CARD NUMBER
1234
1301
RELAY INFORMATION
1303
OBTAIN CARD NUMBER, PUT ACCEPT NUMBER, AND SET ENCRYPTION METHOD
1304
OBTAIN ACCEPT NUMBER AND ENCRYPTION METHOD
ACCEPT NUMBER: 4912
CARD NUMBER: 1234
ACCEPT PROCESSES (11) ~ (14)
4912
MULTIPLY PASSWORD BY 3 AND SUBTRACT 99 FROM RESULT BY ENCRYPTION METHOD
GENERATE AND DISTRIBUTE APPLET
1305
AUTHENTICATION PROCESSES (1), (2)
1306
ACCEPT PROCESSES (15) ~ (17)
AUTHENTICATION PROCESS (7)
ENCRYPT PASSWORD BY APPLET AND TRANSMIT ENCRYPTED PASSWORD
AUTHENTICATION PROCESSES (3) ~ (5)
1307
AUTHENTICATION PROCESS (6)
1308
PASSWORD: 9104
ENCRYPTED PASSWORD: 27213
OBTAINED ENCRYPTED PASSWORD
USER INPUTTING FROM INTERMEDIARY SERVER AND OBTIANING ENCRRYPTED PASSWORD
1309
CONFIRM ENCRYPTION METHOD
AUTHNETICATION PROCESSES (8) ~ (10)
ENCRYPTED PASSWORD: 27213
READ TARGET DATA
ENCRYPTED PASSWORD: 27213
1310
CARD NUMBER: 1234. PASSWORD: 9104
AUTHENTICATION PROCESS (11)
1311
ENCRYPT PASSWORD
1312
AUTHENTICATION PROCESSES (12) ~ (17)
ENCRYPTED PASSWORD: 27213
AUTHENTICATION PROCESSES (18) ~ (20)
1313
COLLATE PASSWORD IN DB WITH INPUTTED PASSWORD (BOTH ARE GIVEN IN CIPHER MODE)
1314
PROVIDE INFORMATION
OBTAIN INFORMATION
AUTHENTICATION IS ESTABLISHED IF IDENTICAL WITH 27213

FIG. 14

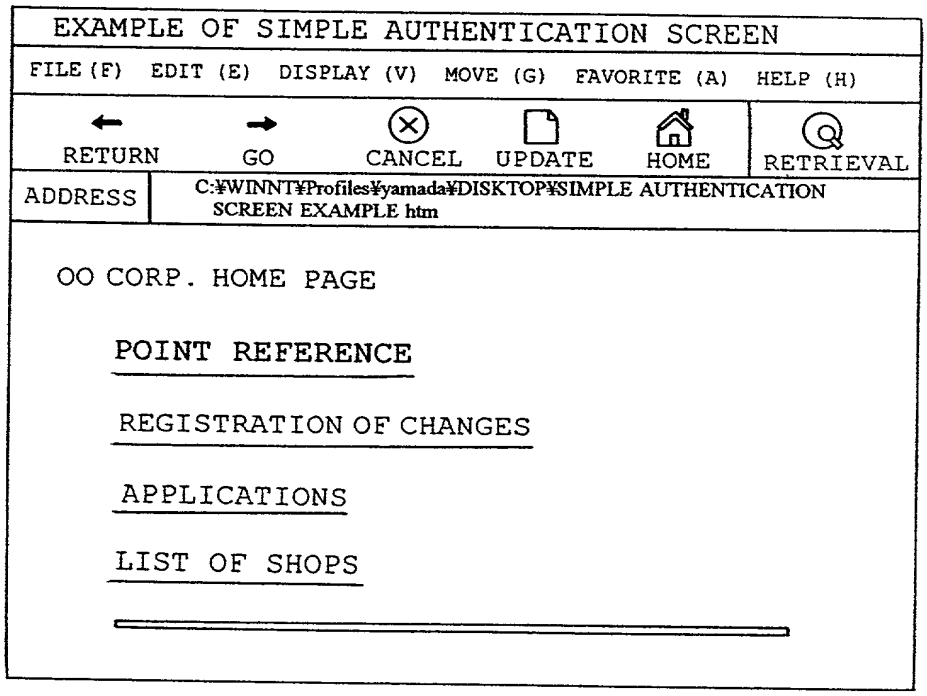

EXAMPLE OF SIMPLE AUTHENTICATION SCREEN
FILE (F) EDIT (E) DISPLAY (V) MOVE (G) FAVORITE (A) HELP (H)
RETURN
GO
CANCEL
UPDATE
HOME
RETRIEVAL
ADDRESS
C:¥WINNT¥Profiles¥yamada¥DISKTOP¥SIMPLE AUTHENTICATION SCREEN EXAMPLE htm
OO CORP. HOME PAGE
POINT REFERENCE
REGISTRATION OF CHANGES
APPLICATIONS
LIST OF SHOPS

FIG. 15

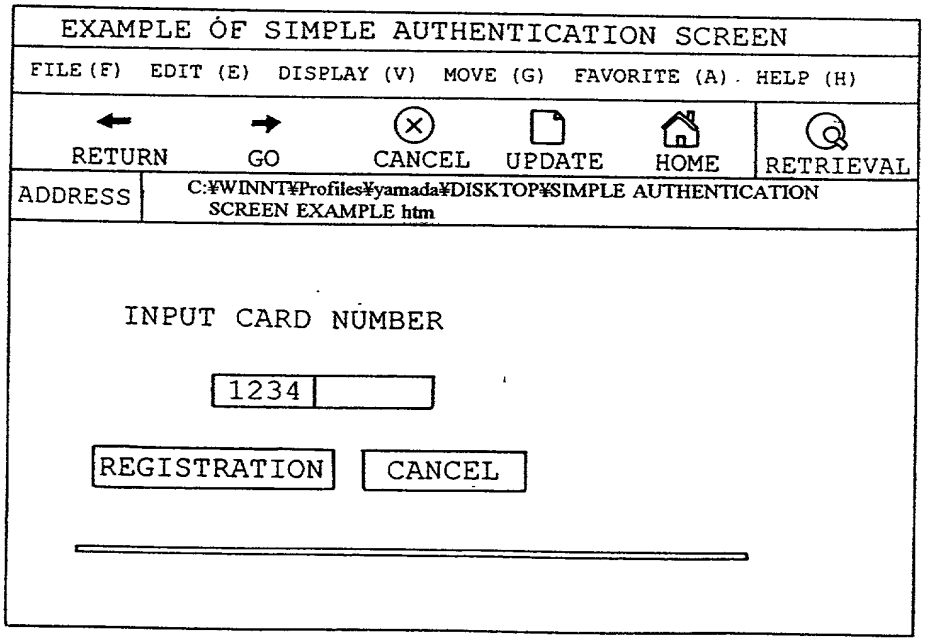

EXAMPLE OF SIMPLE AUTHENTICATION SCREEN
FILE (F) EDIT (E) DISPLAY (V) MOVE (G) FAVORITE (A) HELP (H)
RETURN
GO
CANCEL
UPDATE
HOME
RETRIEVAL
ADDRESS
C:¥WINNT¥Profiles¥yamada¥DISKTOP¥SIMPLE AUTHENTICATION SCREEN EXAMPLE htm
INPUT CARD NUMBER
1234
REGISTRATION
CANCEL

FIG. 16

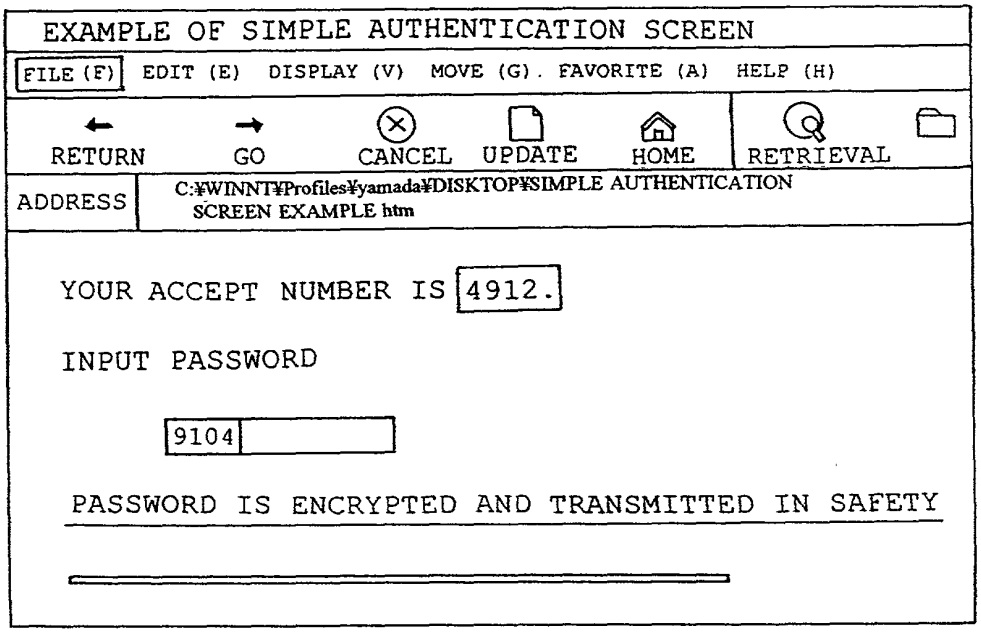

EXAMPLE OF SIMPLE AUTHENTICATION SCREEN
FILE (F) EDIT (E) DISPLAY (V) MOVE (G). FAVORITE (A) HELP (H)
RETURN
GO
CANCEL
UPDATE
HOME
RETRIEVAL
ADDRESS
C:¥WINNT¥Profiles¥yamada¥DISKTOP¥SIMPLE AUTHENTICATION SCREEN EXAMPLE htm
YOUR ACCEPT NUMBER IS 4912.
INPUT PASSWORD
9104
PASSWORD IS ENCRYPTED AND TRANSMITTED IN SAFETY

FIG. 17

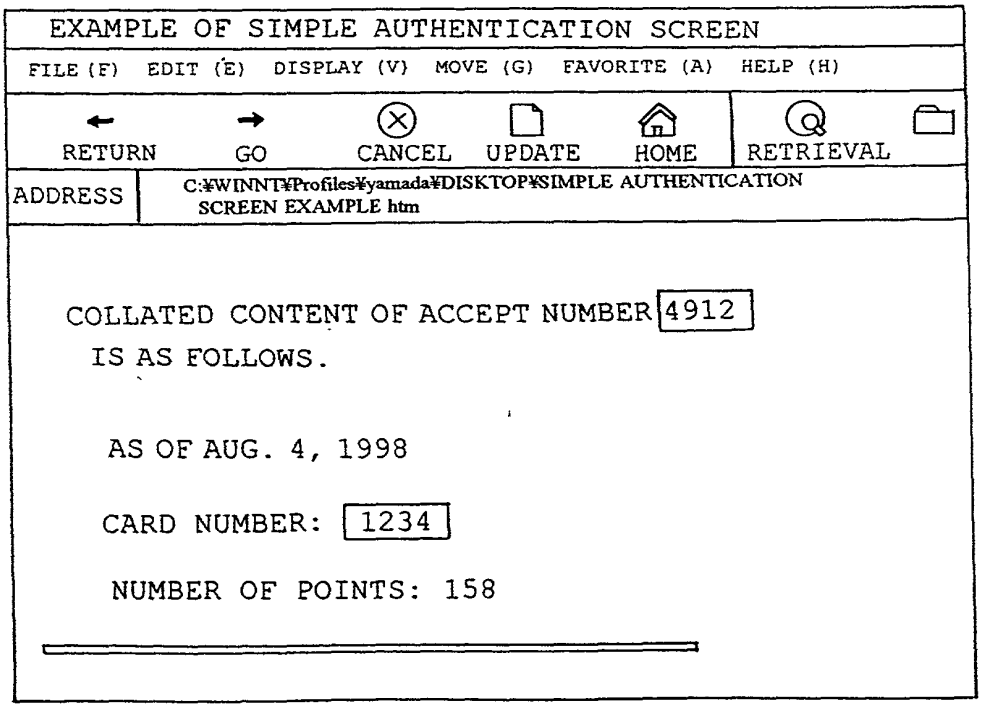

EXAMPLE OF SIMPLE AUTHENTICATION SCREEN
FILE (F) EDIT (E) DISPLAY (V) MOVE (G) FAVORITE (A) HELP (H)
RETURN
GO
CANCEL
UPDATE
HOME
RETRIEVAL
ADDRESS
C:¥WINNT¥Profiles¥yamada¥DISKTOP¥SIMPLE AUTHENTICATION SCREEN EXAMPLE htm
COLLATED CONTENT OF ACCEPT NUMBER 4912
IS AS FOLLOWS.
AS OF AUG. 4, 1998
CARD NUMBER: 1234
NUMBER OF POINTS: 158

FIG. 18

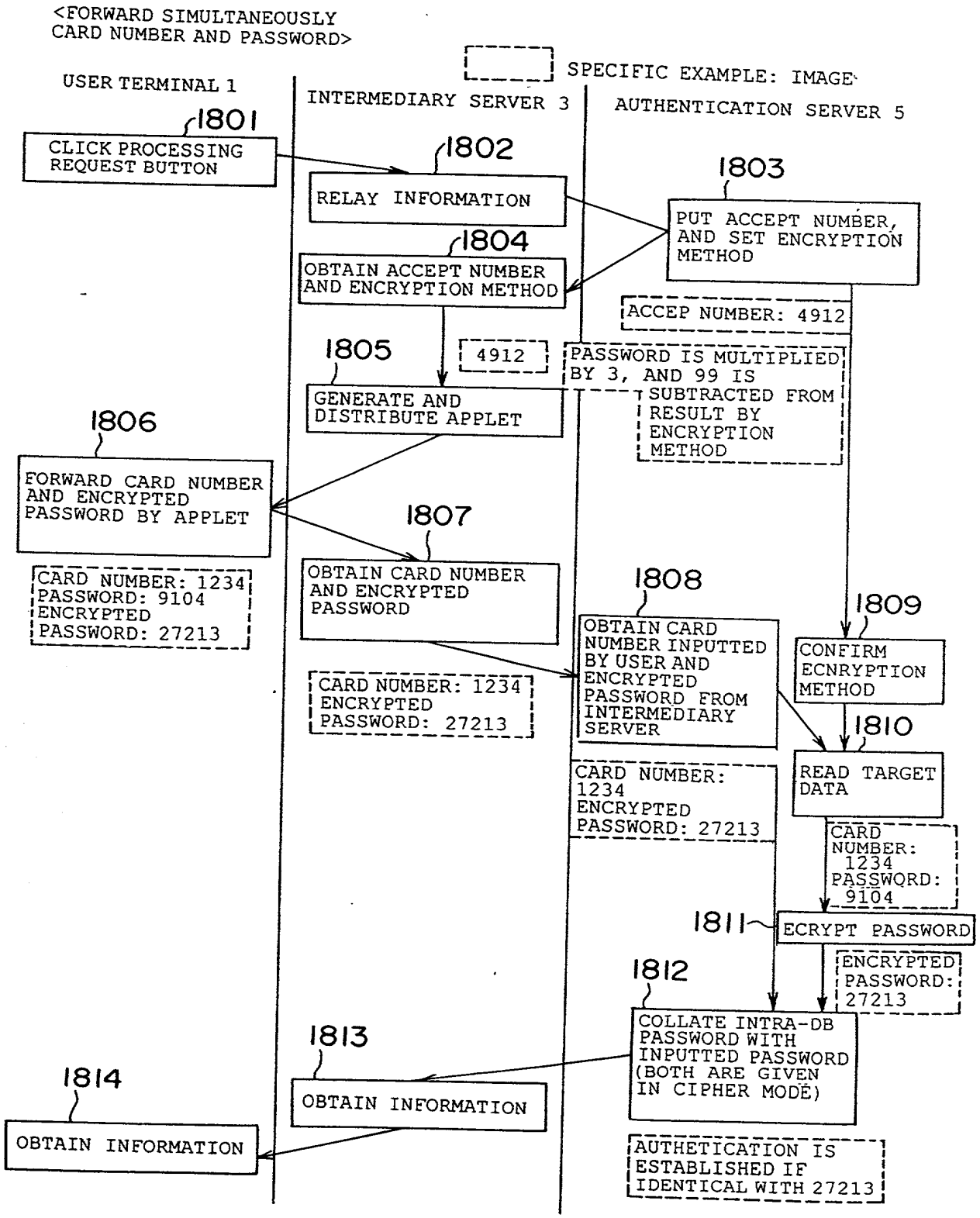
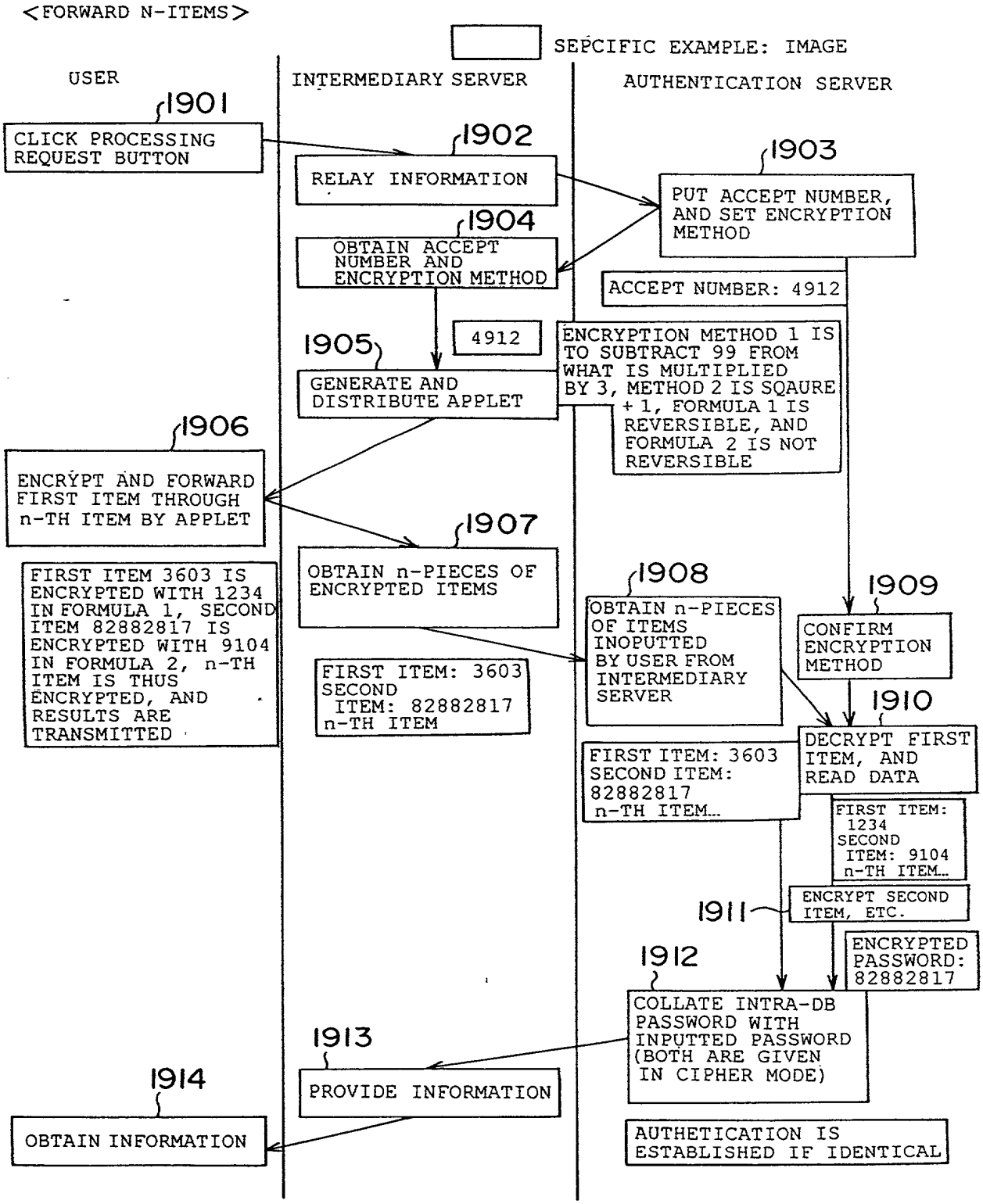

<FORWARD SIMULTANEOUSLY CARD NUMBER AND PASSWORD>
SPECIFIC EXAMPLE: IMAGE
USER TERMINAL 1
INTERMEDIARY SERVER 3
AUTHENTICATION SERVER 5
1801
CLICK PROCESSING REQUEST BUTTON
1802
RELAY INFORMATION
1803
PUT ACCEPT NUMBER, AND SET ENCRYPTION METHOD
1804
OBTAIN ACCEPT NUMBER AND ENCRYPTION METHOD
ACCEP NUMBER: 4912
1805
4912
PASSWORD IS MULTIPLIED BY 3, AND 99 IS SUBTRACTED FROM RESULT BY ENCRYPTION METHOD
GENERATE AND DISTRIBUTE APPLET
1806
FORWARD CARD NUMBER AND ENCRYPTED PASSWORD BY APPLET
CARD NUMBER: 1234 PASSWORD: 9104 ENCRYPTED PASSWORD: 27213
1807
OBTAIN CARD NUMBER AND ENCRYPTED PASSWORD
1808
OBTAIN CARD NUMBER INPUTTED BY USER AND ENCRYPTED PASSWORD FROM INTERMEDIARY SERVER
1809
CONFIRM ECNRYPTION METHOD
CARD NUMBER: 1234 ENCRYPTED PASSWORD: 27213
1810
READ TARGET DATA
CARD NUMBER: 1234 PASSWORD: 9104
1811
ECRYPT PASSWORD
ENCRYPTED PASSWORD: 27213
1812
COLLATE INTRA-DB PASSWORD WITH INPUTTED PASSWORD (BOTH ARE GIVEN IN CIPHER MODE)
AUTHETICATION IS ESTABLISHED IF IDENTICAL WITH 27213
1813
OBTAIN INFORMATION
1814
OBTAIN INFORMATION

FIG. 19


<FORWARD N-ITEMS>
SEPCIFIC EXAMPLE: IMAGE
USER
INTERMEDIARY SERVER
AUTHENTICATION SERVER
1901
CLICK PROCESSING REQUEST BUTTON
1902
RELAY INFORMATION
1903
PUT ACCEPT NUMBER, AND SET ENCRYPTION METHOD
1904
OBTAIN ACCEPT NUMBER AND ENCRYPTION METHOD
ACCEPT NUMBER: 4912
4912
1905
GENERATE AND DISTRIBUTE APPLET
ENCRYPTION METHOD 1 IS TO SUBTRACT 99 FROM WHAT IS MULTIPLIED BY 3, METHOD 2 IS SQAURE + 1, FORMULA 1 IS REVERSIBLE, AND FORMULA 2 IS NOT REVERSIBLE
1906
ENCRYPT AND FORWARD FIRST ITEM THROUGH n-TH ITEM BY APPLET
1907
OBTAIN n-PIECES OF ENCRYPTED ITEMS
1908
OBTAIN n-PIECES OF ITEMS INOPUTTED BY USER FROM INTERMEDIARY SERVER
1909
CONFIRM ENCRYPTION METHOD
FIRST ITEM 3603 IS ENCRYPTED WITH 1234 IN FORMULA 1, SECOND ITEM 82882817 IS ENCRYPTED WITH 9104 IN FORMULA 2, n-TH ITEM IS THUS ENCRYPTED, AND RESULTS ARE TRANSMITTED
FIRST ITEM: 3603 SECOND ITEM: 82882817 n-TH ITEM
1910
DECRYPT FIRST ITEM, AND READ DATA
FIRST ITEM: 3603 SECOND ITEM: 82882817 n-TH ITEM...
FIRST ITEM: 1234 SECOND ITEM: 9104 n-TH ITEM...
1911
ENCRYPT SECOND ITEM, ETC.
ENCRYPTED PASSWORD: 82882817
1912
COLLATE INTRA-DB PASSWORD WITH INPUTTED PASSWORD (BOTH ARE GIVEN IN CIPHER MODE)
1913
PROVIDE INFORMATION
1914
OBTAIN INFORMATION
AUTHETICATION IS ESTABLISHED IF IDENTICAL

Docket No. 108269-00005 ARENT FOX KINTNER PLOTKIN & KAHN, PLLC

Declaration For U.S. Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention **entitled**
(Insert Title) NETWORK AUTHENTICATION SYSTEM AND METHOD THEREOF
the specification of which is attached hereto unless the following box is checked:

☒ was filed on November 15, 1999 as PCT International Application Number PCT/JP99/06365
and was amended on _____ **and/or** was filed on _____
as United States Application Number _____ and was amended on _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designates at least one country other than the United States, listed below and have also identified below any foreign application(s) for patent or inventor's certificate or PCT International Application having a filing date before that of the application for which priority is claimed:

(List prior foreign applications. See note A on back of this page)	(Number)	(Country)	(Day/Month/Year Filed)	Priority Claimed
	10-343 565	Japan	16 / 11 / 98	☒ Yes ☐ No
				☐ Yes ☐ No
				☐ Yes ☐ No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)

(See Note B on back of this page) ☐ See attached list for additional prior foreign or provisional applications.

I hereby claim the benefit under 35 U.S.C. §120 of any United States application(s) or §365(c) of any PCT International application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior application(s) (U.S. or PCT) in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. §1.56 which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

(List prior U.S. Applications or PCT International applications designating the U.S.)	(Application Serial No)	(Filing Date)	(Status) (patented, pending, *abandoned*)

And I hereby appoint the firm of Arent Fox, Customer Number **004372** including as principal attorneys: David T. Nikaido, Reg. No. 22,663; Charles M. Marmelstein, Reg. No. 25,895; George E. Oram, Jr., Reg. No. 27,931; Robert B. Murray, Reg. No. 22,980; Douglas H. Goldhush, Reg. No. 33,125; Richard J. Berman, Reg. No. 39,107; Murat Ozgu, Reg. No. 44,275; Robert K. Carpenter, Reg. No. 34,794; Gregory B. Kang, Reg. No. 45,273; Rustan J. Hill, Reg. No. 37,351; Rhonda L. Barton, Reg. No. 47,271; Carl Schaukowitch, Reg. No. 29,211; Kevin F. Turner, Reg. No. 43,437; Hans J. Crosby, Reg. No. 44,634; and Brian A. Tollefson, Reg. No. 46,338.

Please direct all communications to the following address: ARENT FOX KINTNER PLOTKIN & KAHN, PLLC
1050 Connecticut Avenue, N.W., Suite 600
Washington, D.C. 20036-5339
Tel: (202) 857-6000; Fax: (202) 638-4810

The undersigned hereby authorizes the U.S. attorneys named herein to accept and follow instructions from the undersigned's assignee, if any, and/or, if the undersigned is not a resident of the United States, the undersigned's domestic attorney, patent attorney or patent agent, as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorneys and the undersigned. In the event of a change in the person(s) from whom instructions may be taken, the U.S. attorneys named herein will be so notified by the undersigned.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(See Note C on back of this page)

Full name of sole or first inventor Kazuhiro AIHARA

Inventor's signature Kazuhiro Aihara July 19, 2001
Date

Residence Tokyo, Japan JPX

Citizenship Japanese

Post Office Address c/o Saison Information Systems Co., Ltd., 44-3, Higashiikebukuro 1-chome, Toshima-ku, Tokyo 171-0013, Japan

Full name of second joint inventor, if any Kuniaki TANEZAKI

Inventor's signature Kuniaki Tanezaki July 19, 2001
Date

Residence Saitama, Japan JPX

Citizenship Japanese

Post Office Address Aruru Oomiya 305, 56-6, Konba-chou, Oomiya-shi, Saitama-ken, 330-0032, Japan

Full name of third joint inventor, if any Masakatsu TSUKAMOTO

Inventor's signature Masakatsu Tsukamoto July 19, 2001
Date

Residence Tokyo, Japan JPX

Citizenship Japanese

Post Office Address c/o Saison Information Systems Co., Ltd., 44-3, Higashiikebukuro 1-chome, Toshima-ku, Tokyo 171-0013, Japan

Full name of fourth joint inventor, if any Tamami YAMADA

Inventor's signature Tamami Yamada July 19, 2001
Date

Residence Tokyo, Japan JPX

Citizenship Japanese

Post Office Address Virunuubu Hachiouji 208, 3-17-6, Myoujin-chou, Hachiouji-shi, Tokyo 192-0046, Japan

Full name of fifth joint inventor, if any

Inventor's signature _____ Date

Residence

Citizenship

Post Office Address

Full name of sixth joint inventor, if any

Inventor's signature _____ Date

Residence

Citizenship

Post Office Address

Full name of seventh joint inventor, if any

Inventor's signature _____ Date

Residence

Citizenship

Post Office Address

Full name of eighth joint inventor, if any

Inventor's signature _____ Date

Residence

Citizenship

Post Office Address

Full name of ninth joint inventor, if any

Inventor's signature _____ Date

Residence

Citizenship

Post Office Address